CHAPTER 9
MAINTENANCE PRACTICES

9-1. General maintenance

A comprehensive maintenance program is critical to attaining long-term reliable performance of SCADA systems. Periodic device calibration, preventive maintenance, and testing allow potential problems to be identified before they can cause mission failure. Prompt corrective maintenance assures reliability by minimizing downtime of redundant components.

9-2. Preventive maintenance

The SCADA system should be part of the overall preventive maintenance (PM) program for the facility. Table 9-1 provides a list of recommended maintenance activities and frequencies for SCADA systems and their components. Preventive maintenance schedules for SCADA components and subsystems should be coordinated with those for the mechanical/electrical systems they serve to minimize overall scheduled downtime.

Table 9.1 Recommended maintenance activities.

Activity	Frequency
Pneumatic Systems/Components	
Check Regulators and Filters	Monthly
Inspect Tubing and Piping	Monthly
Actuate Pressure Switches	6 Months
Actuate (Stroke) Valves and Actuators	6 Months
Calibrate Switches and Sensors	Yearly
Calibrate Pressure Gauges	Yearly
Calibrate Thermometors	Yearly
Electrical/Electronic Systems	
Lamp Test/Verify Indicators	Monthly
Inspect Enclosures for Dirt, Water, Heat	Monthly
Actuate (Stroke) Valves and Actuators	6 Months
Actuate Switches	6 Months
Run PLC Diagnostics	6 Months
Calibrate Sensors and Transmitters	Yearly
Calibrate Meters	Yearly
Calibrate Actuators	Yearly
Test Batteries	6 Months
Test Automatic control Sequences	Yearly
Verify Alarms	Yearly
Software Maintenance and Patching	2 Months
Anti-virus Definition Updates	Monthly
Inspect Wire, Cable and Connections	Monthly

   a. Many components of SCADA systems, such as dead-bus relays, are not required to function under normal system operating modes. For this reason the system should be tested periodically under actual or simulated contingency conditions. These tests should approach as closely as possible the actual off-

normal conditions in which the system must operate. For example, SCADA for standby generator plants should be tested by interrupting the utility source as far upstream of the normal service as possible.

b. Periodic system testing procedures can duplicate or be derived from the functional performance testing procedures discussed in chapter 8.

c. The SCADA software maintenance should include timely updates of any new versions from the supplier and testing to verify proper installation on the SCADA computer. In addition, software anti-virus updates should be maintained. This should be performed any time after the computer is connected to the Internet. Normal operation requires that the SCADA computer not be connected to the Internet.

d. Electrical power systems, both AC and DC, serving SCADA systems should be maintained in accord with the requirements of TM 5-692-1 and NFPA 70B.

9-3. Concurrent maintenance

Concurrent maintenance is defined as testing, troubleshooting, repair or replacement of a component or subsystem while redundant component(s) or subsystem(s) are serving the load. The ability to perform concurrent maintenance is critical to attaining the specified reliability/availability criteria for C4ISR facilities and must be designed into the SCADA system. Where SCADA components are associated with equipment that has redundancy and therefore are not themselves redundant, their maintenance should be scheduled to occur during maintenance of the associated equipment. SCADA components and controllers that are redundant must be capable of being taken out of service, repaired or replaced and tested without interfering with the operation of the redundant component.

9-4. Reliability centered maintenance

Reliability-Centered Maintenance (RCM) is an approach for developing an effective and efficient maintenance program based on the reliability characteristics of the constituent parts and subsystems, economics, and safety. RCM provides a logical, structured framework for determining the optimum mix of applicable and effective maintenance activities needed to sustain the operational reliability of systems and equipment while ensuring their safe and economical operation and support. RCM has changed the approach to preventive maintenance, and can be considered the "next step" in moving from a trial and error based approach to establishing PM frequencies to an intelligent approach to maintenance planning. A significant byproduct of the application of SCADA systems to the control of C4ISR facilities is the large amount of operational data made available through the trending and data storage features of the SCADA. This operational data can be used for automated performance monitoring of mechanical and electrical systems that can support a RCM approach. Detailed information about the application of RCM to C4ISR facilities can be found in Chapter 3 of TM 5-698-1, and in TM 5-698-2.

9-5. Operations and maintenance documentation

The design agency should perform an O&M analysis to determine the O&M data required to support maintenance of the SCADA system by the using government agency. This analysis should be coordinated with the using government agency to determine maintenance parameters and O&M data that are available to the using government agency. Typical O&M data requirements include the following items:

a. System documentation as defined in chapter 10.

b. Minimum spare parts list.

c. Recommended spare parts list.

d. Recommended onsite test equipment.

e. Recommended O&M training.

f. Recommended O&M to be performed by contract.

9-6.   Spare parts stocking

An adequate on-site stock of spare parts is essential to obtaining high availability of SCADA systems. Reliability calculations demonstrating compliance with "six nines" criteria typically use repair times based on "replace with spare" which are shorter than those for "repair failed component". If on-site stocks are inadequate, actual availabilities will be significantly less than these calculated values.

a. Minimum recommended stocking levels include the following. These quantities may need to be increased for components which are used in large numbers in the facility:

(1)   Manufacturer's recommended spare parts list.

(2)   One each of all line replaceable boards or modules.

(3)   Six each power and control fuses used in the system.

(4)   Tools required to terminate coaxial on fiber optic cables.

b. Specifications should also require that the following be furnished with each system:

(1)   Laptop computer loaded with software required to access controllers.

(2)   Licenses for all software installed on the system.

(3)   Permission to modify program code.

(4)   Spare cables for connecting computer to controllers.

9-7. Technical support

The design agency should specify functional areas of the operating system and/or equipment where a technical representative will be furnished by the manufacturer for training, test, checkout, validation, or pre-operational exercises. Ongoing O&M of SCADA system software may require technical support from the system vendor or from agency technical personnel not located at the facility. Commercial SCADA software typically has provisions for remote modem access that permit this type of support from the vendor's location or an agency central engineering group. Such remote access provisions represent a vulnerability to "hacking" and must be used with great caution. They should be monitored when in use and physically disconnected when not in use. PLC suppliers have indicated that they are unable to provide a firewall that will protect the controller program in the event of unauthorized access to the HMI processor. Password protection policies for all SCADA systems, including PLC's, shall be in compliance with established DoD policies. The DoD policy is established by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01 D, Information Assurance (AI) and Computer Network Defense (CND).

These policies require that the default password that came from the control supplier be changed when placed into operation at the facility.